SPA Using ZTNA Deployment Guide

FortiSASE

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Change log

Date	Change description
2024-05-09	Initial release.
2024-05-21	Updated: • Use cases and topology on page 10 • Design concept and considerations on page 11 • Appendix B - Documentation references on page 29

Introduction

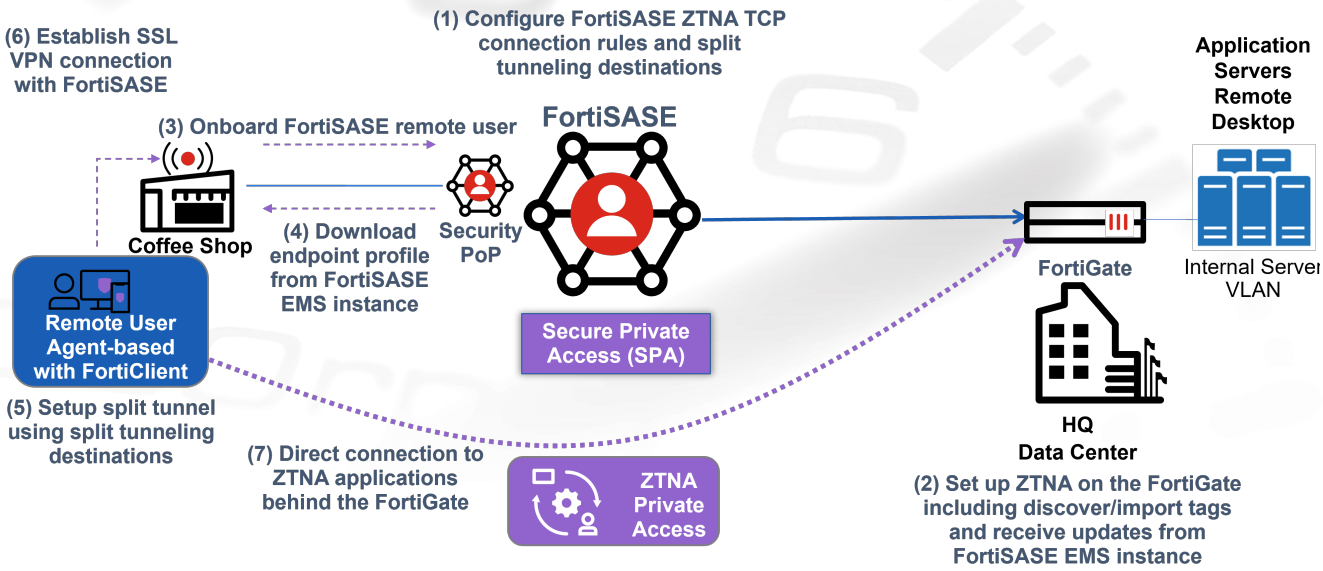
This document describes Fortinet's recommended approach to configuring our secure private access (SPA) solution for FortiSASE using zero trust network access (ZTNA). It covers configuration of the solution.

Executive summary

In today's remote workforce, a remote worker requires secure access to the following primary locations: the corporate network, applications in the cloud, and the rest of the internet. Secure access service edge (SASE) solutions such as FortiSASE provide the means to secure the cloud and the internet, but most corporations want a seamless integration between securing the public network and their private network.

This guide examines how FortiSASE can integrate with FortiGate ZTNA to provide a seamless experience for end users while securing your most important corporate assets behind the FortiGate application gateway. Unlike traditional SSL and IPsec VPN, FortiSASE SPA using ZTNA offers direct connections to protected resources without requiring establishment of a persistent tunnel. The key to ZTNA is verifying the connecting device's and user's identities and ensuring the device's security posture before admitting it to the protected network. These security checks happen instantly and transparently thanks to the integration between FortiSASE, FortiGate, and the FortiClient endpoint. If a device cannot pass these security checks, it is considered untrusted and the connection is rejected.

The following illustrates the architecture of the FortiSASE, FortiGate, and FortiClient integration.



This guide explores the setup between FortiSASE and your corporate FortiGate firewall in detail to cover the SPA using ZTNA use case. It first reviews the components in this solution to understand more about the inner workings, then dives into design concepts and considerations. Finally, it steps through a deployment scenario to build a working FortiSASE and ZTNA environment.

Intended audience

This guide is intended for a technical audience, including system and network architects, design engineers, network engineers, and security engineers who want to deploy FortiSASE to secure their remote workers while integrating with their FortiGate ZTNA solution to remotely access their network with the goal of providing SPA.

The solution in this guide is targeted at small- and medium-sized organizations and enterprises.

This guide assumes that the reader is familiar with basic concepts of applications, networking, routing, security, and proxies, and has a basic understanding of network and data center architectures.

For comments and feedback about this document, visit FortiSASE Endpoint with ZTNA Shortcuts Deployment on community.fortinet.com.

About this guide

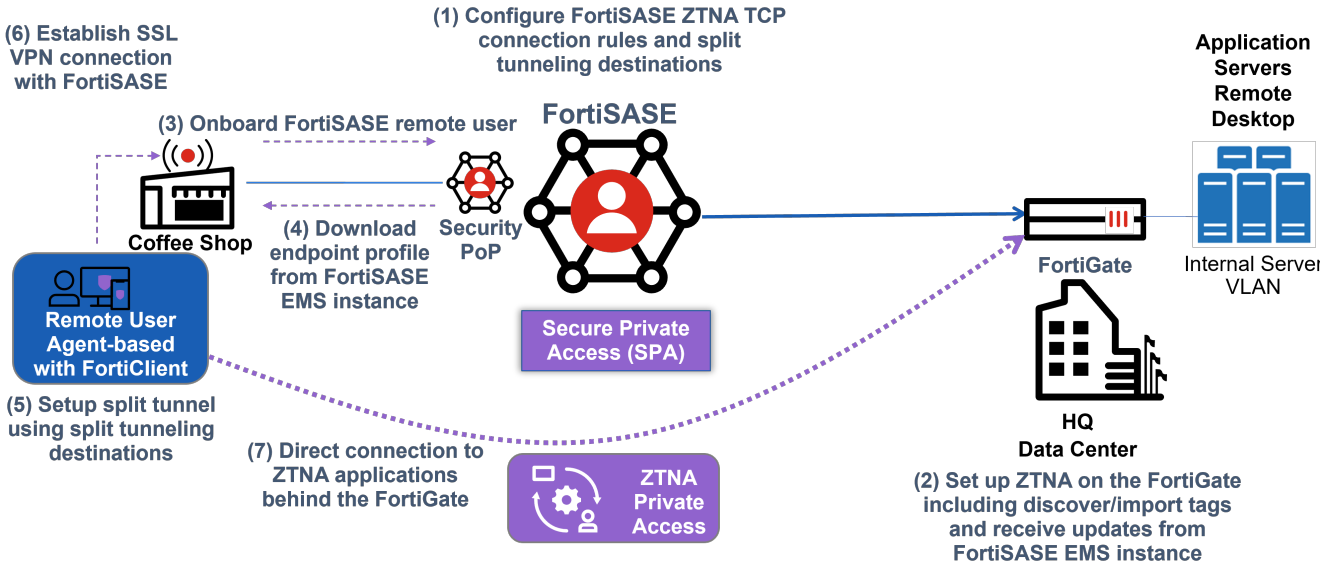
The deployment guide serves the purpose of going through the design and deployment steps involved in deploying a specific architecture. Readers should first evaluate their environments to determine whether the architecture and design that this guide outlines suits them.

Where appropriate, reviewing supplementary material in product admin guides, example guides, cookbooks, release notes, and other documents is recommended.

Solution overview

FortiSASE with ZTNA architecture

You are likely familiar with the FortiSASE endpoint solution. FortiSASE provides secure internet access to end users who are registered and connected to FortiSASE. With further integration, FortiSASE can also share endpoint information with a FortiGate. This allows the corporate FortiGate to implement zero trust network access (ZTNA) for remote users who are already registered to FortiSASE, which, therefore, provides them with secure private access to private applications behind the corporate FortiGate. The following diagram outlines the high-level communication between FortiSASE, FortiGate, and FortiClient to deliver an integrated FortiSASE and ZTNA solution.



Zero trust

Trust is at the core of the ZTNA solution. Traditionally, organizations allow remote users to access corporate resources through VPNs based on their user identity. Once authentication succeeds, the users are trusted to access any resources allowed for their user group for the duration of their VPN connection.

Zero trust, on the other hand, does not solely rely on user identity but also verifies other attributes in real time. These attributes include the endpoint's device identity and security posture. A client certificate that a trusted certificate authority (CA) generated uniquely identifies an endpoint that the certificate is assigned to. The FortiGate uses the certificate to verify device identity. The FortiGate determines the device's security posture using security attributes called ZTNA tags, which the endpoint shares with FortiSASE and the FortiGate. Examples include detecting any of the following:

- Whether a device has antivirus installed
- Whether a device has critical vulnerabilities patched
- Whether FortiClient detects any malware on the device

A Zero Trust security device, the FortiGate in this case, must establish a trust context with the endpoint based on these attributes. The FortiGate continues to evaluate this trust context when allowing the device to access protected resources. If any attribute changes and the device becomes untrusted, the FortiGate terminates the sessions.

FortiClient, FortiSASE, and FortiGate architecture

To understand how real-time ZTNA functions in the FortiSASE with ZTNA solution, the following breaks down the roles that each component plays in this architecture:

FortiClient

When a FortiSASE endpoint registers to FortiSASE, it provides device information, such as network details, operating system, and logged-on user to FortiSASE. It also synchronizes the endpoint profile from FortiSASE and provides information about its current security posture. When FortiClient detects changes to an attribute, such as detecting a critical vulnerability, it reports the status to FortiSASE.

Upon initial registration, FortiClient requests and obtains a client device certificate from the FortiSASE ZTNA certificate authority. The client device uses this certificate to identify itself to the FortiGate.

FortiSASE

FortiSASE issues and signs the client certificate with the FortiClient UID, certificate serial number, and the Endpoint Management Service's serial number. FortiSASE synchronizes the certificate details to the FortiGate. FortiSASE shares its own ZTNA CA certificate with the FortiGate, so that the FortiGate can use it to validate client certificates that the same CA has signed.

FortiSASE defines endpoint tagging rules for tagging each endpoint's important security attributes. FortiSASE pushes the rules through the endpoint profile to FortiClient. Once synchronized, FortiSASE shares these tags and each client's status with the FortiGate. See Endpoint posture check for a list of attributes that FortiSASE can configure.

FortiGate

The FortiGate maintains a continuous connection to FortiSASE to synchronize endpoint device information and security tags. When a device's information changes, FortiClient passes the changes to FortiSASE, which then updates to the FortiGate. The FortiGate can use this information when processing connections from the

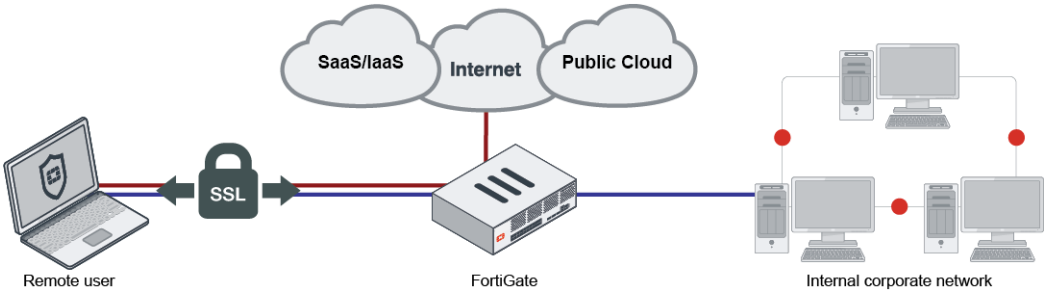
end user to establish the trust context with the endpoint. If an endpoint's security posture change causes it to no longer match the ZTNA policy criteria on an existing session, the FortiGate terminates the session.

Design overview

Use cases and topology

Teleworking via SSL VPN

In a typical teleworking scenario, an organization may use SSL VPN tunneling mode to tunnel all traffic through the FortiGate, including access to the internet and cloud applications. Users may access corporate and web resources based on their user identity for their VPN connection's duration.



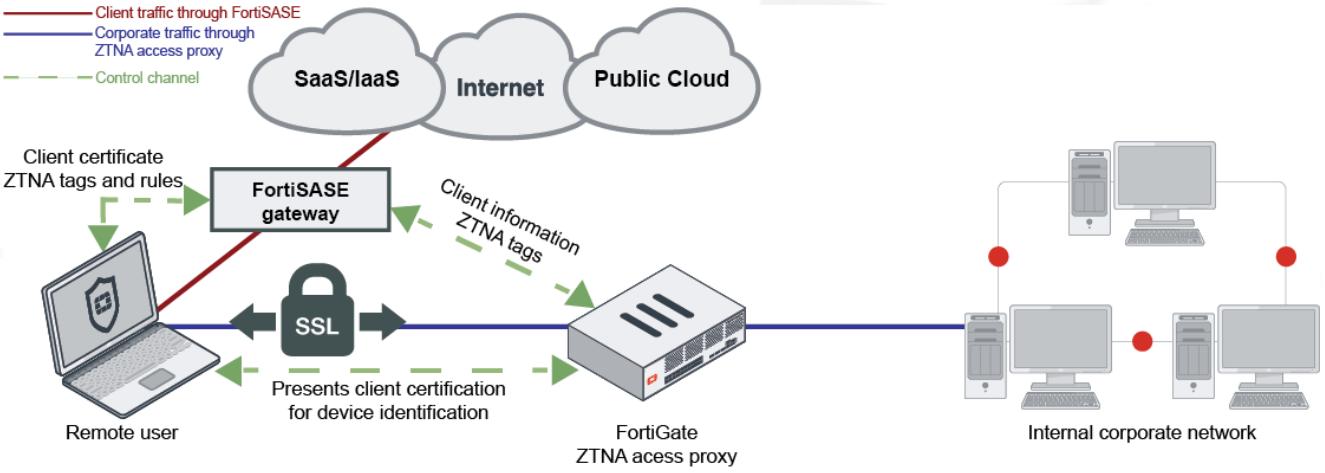
The VPN solution can use security vendors other than Fortinet.

FortiSASE with ZTNA

To offload security for remote workers' direct internet connection to web and cloud resources, you can use FortiSASE. On the other hand, to access corporate resources behind the FortiGate for the secure private access use case, remote users connecting through Zero Trust Network Access (ZTNA) are subject to device identity check, user authentication, and security posture check to ensure that the user and device are trusted.

In FortiSASE FortiClient agent-based mode, a remote computer has the FortiClient agent installed and registered to FortiSASE. When ZTNA integration with the corporate FortiGate is enabled, FortiSASE assigns the FortiClient endpoint a client certificate. You do not need to install an additional application or agent on the remote computer. FortiSASE, FortiClient, and FortiOS transparently synchronize certificates and tags in the background.

When the remote endpoint connects to corporates resources, FortiClient makes an encrypted TCP connection to the FortiGate access proxy. The FortiGate acts as a reverse proxy to serve the requested content. The client-to-FortiGate connection is always encrypted and secured.



Design concept and considerations

FortiSASE endpoint license and configurations

This solution's design uses FortiSASE FortiClient agent-based mode to leverage the use of FortiClient for endpoint registration, SSL VPN, and zero trust network access (ZTNA). Therefore, this solution does not require secure web gateway (SWG) licenses or enabling SWG configuration. This solution only requires endpoint entitlements. Obtain enough FortiSASE endpoint seats to support the number of remote endpoints that will use this service.

FortiGate to FortiSASE connection

To perform ZTNA, you must register the corporate FortiGate to the same FortiCloud account as the FortiSASE instance. This allows the FortiGate's FortiClient EMS Fabric connector to connect to FortiSASE to synchronize endpoint information.

This solution does not support deploying ZTNA with an existing on-premise EMS or FortiClient Cloud instance. You must first provision FortiSASE to allow the FortiGate access proxy to integrate with the FortiSASE Endpoint Management Service.

FortiClient to FortiSASE connection

You must register FortiClient to FortiSASE and maintain this connection to connect to corporate resources through the FortiGate access proxy. When FortiClient disconnects, FortiSASE removes the client certificate from the endpoint, and does not synchronize the client information. The endpoint will not pass client certificate and security posture check against ZTNA.

User management and onboarding

You configure users on FortiSASE for endpoints to authenticate and connect to the FortiSASE gateway. Ideally, users use the same credentials to authenticate to the FortiGate ZTNA access proxy. When designing the solution, consider where users are defined in your organization and use the same authentication source for FortiSASE and FortiGate user configurations. Using local users on either platform is not recommended.

FortiSASE and FortiGate support the following authentication methods:

Method	Description
LDAP user	Configure an LDAP connection and import users and groups from an LDAP server.
RADIUS user	Configure a RADIUS connection and import users and groups from a RADIUS server.
Single sign on (SSO)	Configure a SAML identity provider (IdP) to perform user authentication. FortiSASE and FortiGate act as the SAML service provider (SP).

When you deploy LDAP or RADIUS users for VPN authentication on FortiSASE, you cannot use SSO, and vice-versa.

When using SSO/SAML authentication, your remote endpoint must be able to reach the SAML IdP since the SP redirects users to the IdP to authenticate.

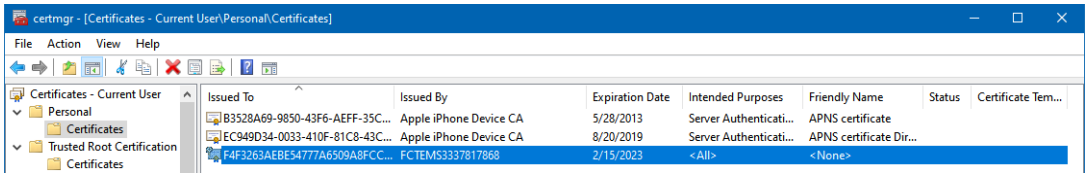
When onboarding remote users, use the *Onboard Users* button to send the invitation code to all remote users. Remote users must install the FortiClient application to use VPN and ZTNA. In larger environments, you should consider using group policy management for Windows or other centralized management systems like mobile device management to centrally manage their FortiClient endpoint deployment.

ZTNA: Client and server CA certificates

When FortiClient registers to FortiSASE, it requests a client certificate to use for device identification. The ZTNA CA installed on the FortiSASE instance issues the certificate.

To view a client certificate on a Windows endpoint:

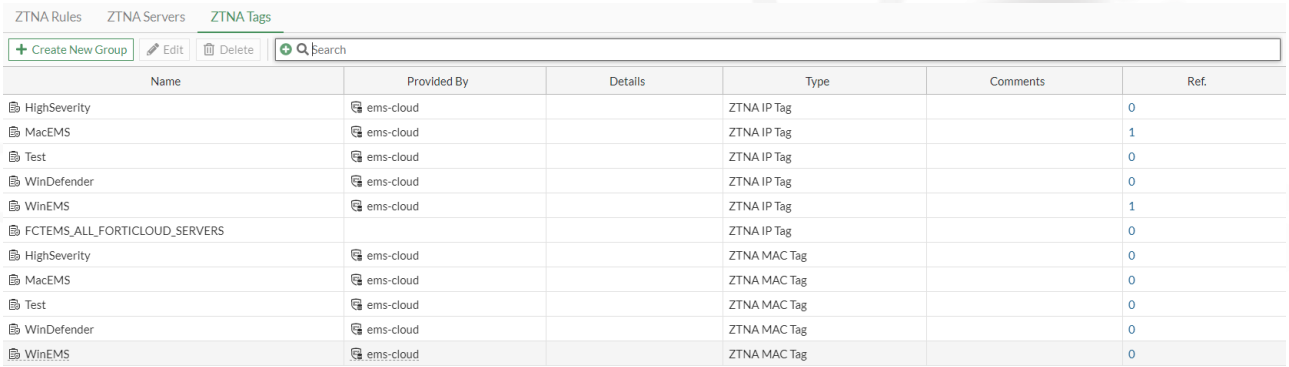
1. In the Windows Start menu, search for and select *Manage user certificates*.
2. In Certificate Manager, go to *Personal* > *Certificates* to view the FortiClient certificate.



ZTNA: Posture check

The FortiGate access proxy performs posture check by verifying the presence or absence of ZTNA tags on a FortiClient endpoint. You define these tags on FortiSASE using tagging rules that specify attributes that can

be checked on the FortiClient endpoint. You should configure these tags and tagging rules carefully, as they determine the basic device security requirements for an endpoint to connect to ZTNA. Design your ZTNA policies with ZTNA tags in mind. You can view synchronized tags in FortiOS in *Policy & Objects > ZTNA > ZTNA Tags*.


ZTNA Rules | ZTNA Servers | ZTNA Tags

+ Create New Group | Edit | Delete | Search

Name	Provided By	Details	Type	Comments	Ref.
HighSeverity	ems-cloud		ZTNA IP Tag		0
MacEMS	ems-cloud		ZTNA IP Tag		1
Test	ems-cloud		ZTNA IP Tag		0
WinDefender	ems-cloud		ZTNA IP Tag		0
WinEMS	ems-cloud		ZTNA IP Tag		1
FCTEMS_ALL_FORTICLOUD_SERVERS			ZTNA IP Tag		0
HighSeverity	ems-cloud		ZTNA MAC Tag		0
MacEMS	ems-cloud		ZTNA MAC Tag		0
Test	ems-cloud		ZTNA MAC Tag		0
WinDefender	ems-cloud		ZTNA MAC Tag		0
WinEMS	ems-cloud		ZTNA MAC Tag		0

See Endpoint posture check for a list of attributes that FortiSASE can configure.

ZTNA: Application list/connection rules

ZTNA connection rules define resources that remote users can access through the ZTNA TCP forwarding access proxy. FortiSASE can push the rules through endpoint profile updates to each FortiClient endpoint. On the endpoint device, when a client tries to access a network resource from these rules, FortiClient listens for connections to the destination resource, namely, the destination address and port, and forwards the connection requests to the FortiGate access proxy. Traffic is encrypted through SSL/TLS between the client and FortiGate, with the underlying traffic to the destination encapsulated within it. In other words, TCP forwarding rules allow the FortiClient to intercept the requests to the destination address and port and forward them to the access proxy.

The encryption option provides encryption between client and FortiGate access proxy for underlying connections that are insecure, like HTTP, FTP, and Telnet. Disabling the encryption option reduces the SSL/TLS encryption overhead for protocols like HTTPS, SSH, and RDP.

FortiGate's HTTP/HTTPS access proxy can allow direct access to a web resource without configuring ZTNA connection rules.

FortiClient: split tunneling destinations

FortiClient establishes a secure connection using SSL VPN to FortiSASE and forwards all traffic to FortiSASE, namely, establishing full tunneling. However, this full tunneling setup poses a challenge with ZTNA TCP forwarding because it means that ZTNA traffic will go to FortiSASE even when a ZTNA destination is being accessed.

Therefore, in FortiSASE, you must configure a split tunneling destination corresponding to the IP or FQDN of the FortiGate ZTNA access proxy to ensure that traffic destined for the ZTNA destination directly uses the internet connection of the endpoint instead of being forwarded to FortiSASE, which is the desired behaviour for ZTNA access.

Deployment overview

This section consists of the following:

Product prerequisites

Customers should obtain enough FortiSASE endpoint seats to support the number of remote endpoints that will use this service.

You must register the FortiGate acting as the Zero Trust Network Access (ZTNA) proxy to the same FortiCloud account as the FortiSASE instance. The FortiGate must be running FortiOS 7.0.5 or a later version to support the latest ZTNA features.

FortiClient endpoints must be running FortiClient 7.0.3 to support ZTNA features.

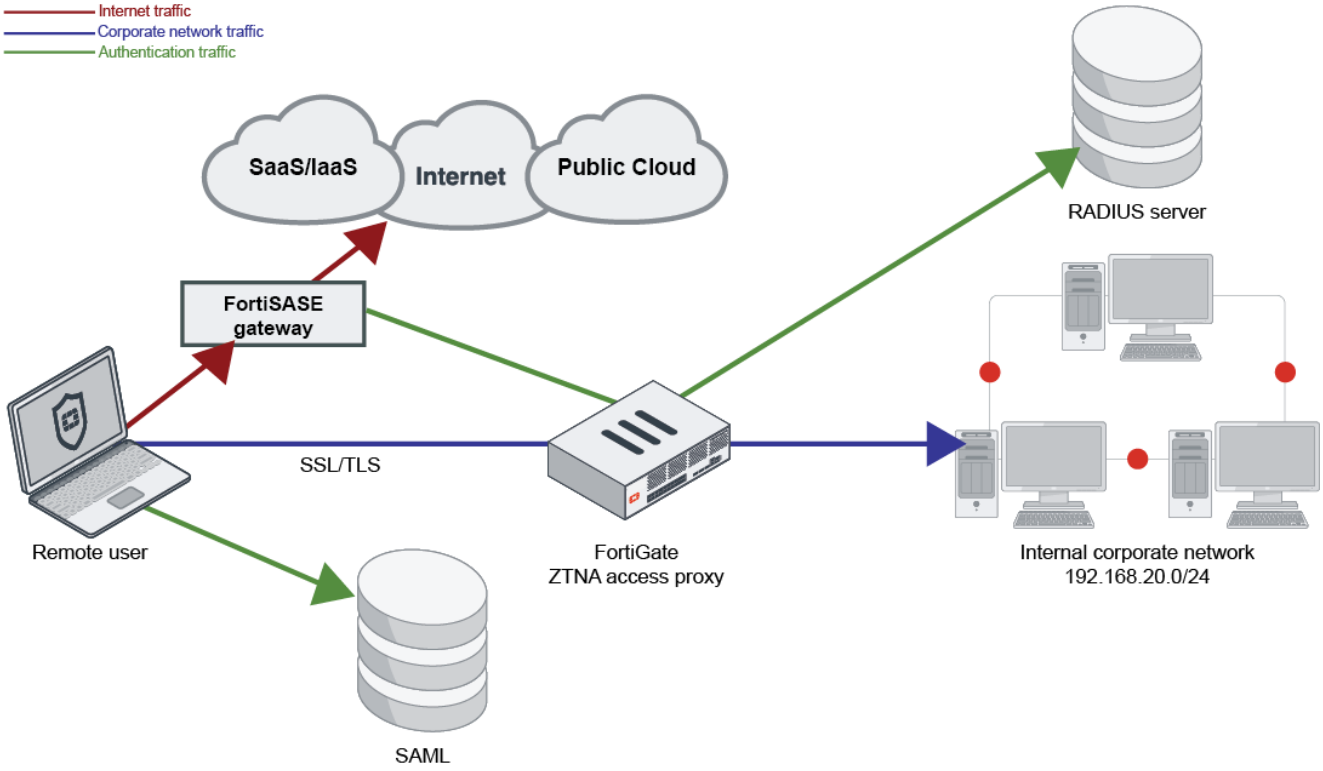
Deployment plan

This outlines the major steps to deploy this solution. Go to Deployment procedures on page 16 for detailed configuration steps:

1. Provision your FortiSASE instance and select the regions where your users will be located. Input licenses as needed. See Provisioning your FortiSASE instance on page 17.
2. Configure remote authentication and onboard users. See Configuring remote authentication and onboarding users on page 17.
3. Configure VPN policies to apply desired scanning and filtering for your users. See Configuring security profiles and policies on page 18.
4. Configure ZTNA tags and tagging rules. See Configuring ZTNA tags and tagging rules on page 19.
5. Connect the FortiGate to FortiSASE over the FortiClient Cloud Fabric connector. Authorize the FortiGate on FortiSASE. FortiSASE automatically synchronizes the tags to the FortiGate. See Connecting the FortiGate to FortiSASE on page 20.
6. On the FortiGate, configure remote authentication servers, authentication schemes, and rules. See Configuring authentication on the FortiGate access proxy on page 21.

7. Configure ZTNA servers. See Configuring ZTNA servers on page 22.
8. Configure ZTNA policies and use user groups and ZTNA tags for access control. See Configuring ZTNA policies on page 22.
9. In FortiSASE, configure ZTNA connection rules to push to clients. See Configuring ZTNA connection rules on FortiSASE on page 23.
10. In FortiSASE, configure a split tunneling destination for the FortiGate ZTNA access proxy to push to clients. See Configuring a split tunneling destination on FortiSASE on page 24.
11. Test and monitor the configuration using a remote device. See Testing and monitoring on page 25.

Deployment procedures



In this sample topology, a FortiSASE instance is deployed and licensed for FortiClient agent-based mode. A FortiGate is configured with Zero Trust Network Access and acts as the access proxy to protect corporate network resources. The FortiGate is registered to the same FortiCloud account as the FortiSASE instance, and receives endpoint information and tags from FortiSASE. The FortiGate is configured with ZTNA policies to allow remote endpoints to access corporate resources. The remote FortiClient endpoint is registered to FortiSASE and synchronizes ZTNA connection rules from it.

The topology displays two authentication sources. When using RADIUS, FortiSASE and FortiGate should point to the same RADIUS server for authentication. When using SAML, you should configure FortiSASE and FortiGate with single sign on and to point to the same SAML identity provider.

You can use the following procedures to provision the aforementioned environment.

Provisioning your FortiSASE instance

Ensure that you have purchased the contract to provision FortiSASE.

To provision your FortiSASE instance:

1. From the Fortinet Support site, register your FortiSASE contract.
2. Once registered, go to *Services* > *Cloud Services* > *FortiSASE* to provision your FortiSASE instance.
3. When provisioning, select the geographic location for your security sites and logging.
4. Once provisioned, the FortiSASE dashboard displays your entitlement in the Remote User Management widget. The number of endpoints that the widget lists is the number of VPN users that are entitled to use this service.

Configuring remote authentication and onboarding users

Depending on the authentication source, the user configuration steps differ. The example shows configuring a RADIUS server and user groups. For configuring other authentication sources, see Authentication Sources and Access.

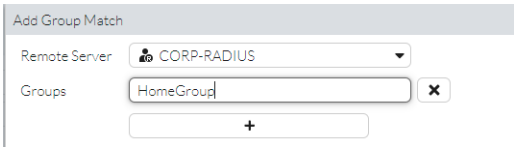
To configure the RADIUS server:

1. Go to *Configuration* > *RADIUS*.
2. Click *Create* to add a new RADIUS server.
   a. Configure the RADIUS server settings:
   b. Enter the desired server name.
   c. Do not enable *Include All Users* unless you want all users on the RADIUS server to be allowed access to FortiSASE.
   d. Click *Next*.
   e. In the *Primary Server* > *IP/Name* field, enter the primary server IP address or fully qualified domain name.
   f. In the *Primary Server* > *Secret* field, enter the primary server secret.
   g. If your organization has a redundant RADIUS server, enter its information in the *Secondary Server* section.
3. Click *Test Connection*.
4. Do one of the following:
   a. If the connection succeeds, click *Next*.
   b. If the connection does not succeed, try again. Confirm your RADIUS server allows traffic from the FortiSASE gateway IP address. This may require sniffing for traffic on port 1812.
5. Review and submit the settings.

To configure a RADIUS user group:

1. Go to *Configuration* > *Users*.
2. Click *Create* > *User Group*.
3. Configure the RADIUS user group(s):
   a. In the *Name* field, enter the desired name.
   b. Under *Remote Groups*, click *Create*.

c. From the *Remote Server* dropdown list, select the RADIUS server that you created.
d. In the *Groups* field, enter the group names of the group(s) that will be allowed access on FortiSASE.



4. Click *OK*.
5. Click *OK* again.
6. A slide-in appears with instructions on how to onboard an end user. Follow the steps under *Managed Endpoint Users > Invite Users* to send invite emails to potential users. Click *Send*. You can also copy the invitation code to share with potential users.
7. Click *Close*.

Configuring security profiles and policies

FortiSASE has a default security profile configured, which is applied to the Allow-All VPN policy. When all users, sources, and destinations require the same scanning and protection, maintaining only one default security profile suffices. However, if different users, sources, or destinations require different protection, create different profile groups for each group of users.

The default VPN policies block any traffic destined for Botnet and C&C servers but allow the rest. Consider your user base and design your VPN policies carefully. FortiSASE matches policies from top down, so add more restrictive policies at the top and less restrictive policies at the bottom.

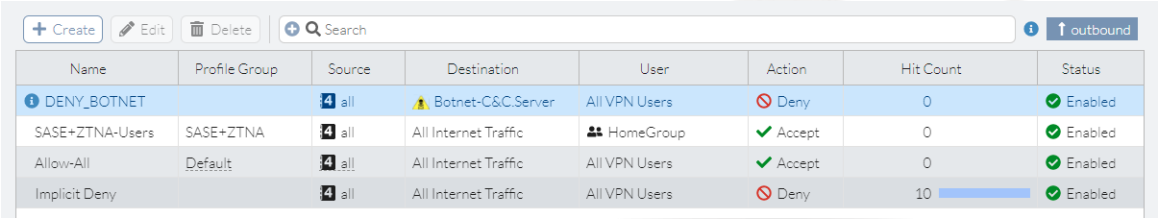
To configure a new security profile:

1. Go to *Configuration > Security*.
2. On the top-right, click the dropdown list beside *Profile Group*, then click *Create*.
3. In the *Create Profile Group* slide-in, enter a name for the new profile.
4. In *Initial Configuration*, select whether to use a basic initial configuration or base the profile on an existing profile.
5. Click *OK*.
6. On the top-right, click the dropdown list again, and select your newly created profile.
7. Edit the profile as desired. See Security for details.

To create a VPN policy:

1. Go to *Configuration > Policies*.
2. Click *Create*.
3. Configure the VPN policy:
   a. In the *Name* field, enter the desired policy name.
   b. For *Source Scope*, select *VPN Users*.
   c. For *Action*, select *ACCEPT*.
   d. In the *Source* field, specify source subnet(s) as desired.
   e. In the *User* field, specify the user group used for your remote users.
   f. In the *Destination* field, specify destination subnet(s) as desired.
   g. In the *Profile Group* field, specify the profile that you created.
   h. In the *Log Allow Traffic* field, select *All Sessions*.

4. Click *OK*.
5. Move the new policy above the Allow-All policy.



Configuring ZTNA tags and tagging rules

Zero Trust Network Access (ZTNA) tags and tagging rules help identify attributes on the endpoints used for posture check on the FortiGate. This example creates two tags: HighSeverity and WinDefender. The goal is to identify whether a Windows endpoint has a high or higher vulnerability status, and whether it has Windows Defender enabled. You will use these tags in the ZTNA policy definition on the FortiGate.

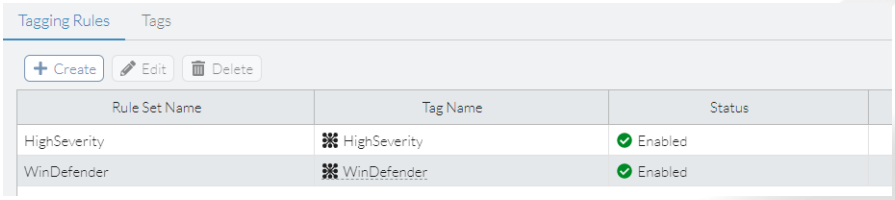
To configure the HighSeverity tag and tagging rule:

1. Go to *Configuration* > *Endpoints* > *ZTNA Tagging* > *ZTNA Tags*. Click *Create*.
2. In the *Name* field, enter HighSeverity. Click *OK*.
3. Go to the *ZTNA Tagging Rules* tab. Click *Create*, and configure the rule:
   a. In the *Name* field, enter HighSeverity.
   b. Under *When the following rules match*, click *Create*.
   c. For *Operating System*, select *Windows*.
   d. From the *Rule Type* dropdown list, select *Severity Level*.
   e. From the *Severity Level* dropdown list, select *High or Higher*.
   f. Click *OK*.
   g. Under *Apply the following tag*, from the *Tag Name* dropdown list, select *HighSeverity*.
   h. Click *OK*.

To configure the WinDefender tag and tagging rule:

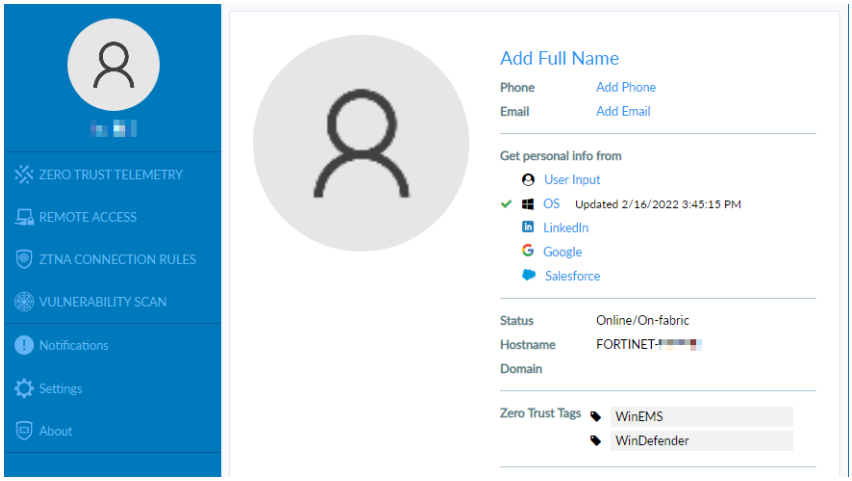
1. Go to *Configuration* > *Endpoints* > *ZTNA Tagging* > *ZTNA Tags*. Click *Create*.
2. In the *Name* field, enter WinDefender. Click *OK*.
3. Go to the *ZTNA Tagging Rules* tab. Click *Create*, and configure the rule:
   a. In the *Name* field, enter WinDefender.
   b. Under *When the following rules match*, click *Create*.
   c. For *Operating System*, select *Windows*.
   d. From the *Rule Type* dropdown list, select *Windows Security*.
   e. From the *Severity Level* dropdown list, select *Windows Defender is enabled*.
   f. Click *OK*.
   g. Under *Apply the following tag*, from the *Tag Name* dropdown list, select *WinDefender*.

h. Click *OK*.



(Optional) To display tags on the FortiClient endpoint:

1. Go to *Configuration* > *Endpoints* > *Profile*.
2. Enable *Show tags on FortiClient*.
3. Click *Apply*. When this option is enabled, detected tags appear on the FortiClient avatar page.



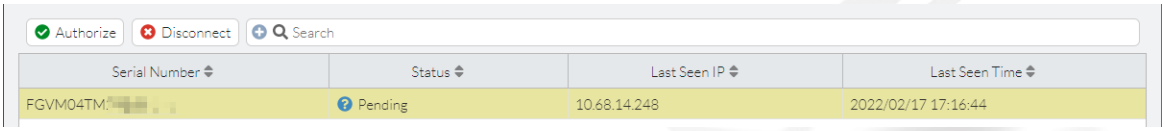
Connecting the FortiGate to FortiSASE

The FortiGate must connect to and be authorized by FortiSASE to synchronize endpoint and tag information.

To connect to FortiSASE from the FortiGate:

1. Verify that the FortiGate is registered to FortiCloud on the same account as FortiSASE:
   a. Go to *System* > *FortiGuard*.
   b. Under *License Information*, verify that FortiCare Support shows the status as registered. Expanding the entry shows the FortiCloud account. Confirm that this account is the account used for FortiSASE.
   c. If the FortiGate is not registered, register now using your FortiCloud account.
2. Go to *Security Fabric* > *Fabric Connectors*.
   a. Click *FortiClient EMS Cloud*.
   b. Ensure that the type is set to *FortiClient EMS Cloud*.
   c. Enter a name for this connection.
   d. Click *OK*. A slide-in appears to verify the server certificate. Accept the certificate.
3. Authorize the FortiGate in FortiSASE:
   a. Go to *Configuration* > *Endpoints* > *ZTNA Access Proxies*.
   b. Select the FortiGate that is pending authorization.

c. Click *Authorize*. Confirm, then click *OK*.



Configuring authentication on the FortiGate access proxy

You should configure the FortiGate with the same remote authentication server as FortiSASE. This example uses RADIUS. To configure other authentication methods, see the FortiOS Admin Guide:

- ZTNA HTTPS access proxy with basic authentication example
- ZTNA proxy access with SAML authentication example

To configure a RADIUS server and user group:

1. Configure a RADIUS server:
   a. Go to *User & Authentication* > *RADIUS Servers*.
   b. Click *Create New*.
   c. Enter the name, IP address/FQDN, and secret for the server.
   d. Click *OK*.
2. Configure a user group:
   a. Go to *User & Authentication* > *User Groups*.
   b. Click *Create New*.
   c. Enter a name, then add a new remote group.
   d. Select the RADIUS server that you created.
   e. Specify the group that was used in the FortiSASE RADIUS configuration. Click *OK*
   f. Click *OK*.

ZTNA requires that an authentication scheme and rule is created to trigger proxy authentication.

To configure an authentication scheme and rule:

1. Go to *System* > *Feature Visibility*. Ensure that the Zero Trust Network Access option is enabled.
2. Configure an authentication scheme:
   a. Go to *Policy & Objects* > *Authentication Rules*.
   b. Click *Create New*, then *Authentication Scheme*.
   c. Enter the desired name.
   d. For *Method*, select *Basic* for configuring Local/RADIUS/LDAP authentication.
   e. For database, select *Other*. Select the RADIUS server created earlier.
   f. Click *OK*.
3. Configure an authentication rule:
   a. In the *Name* field, enter the desired name.
   b. For *Source address*, select *All*.
   c. Leave the *Incoming interface* field blank.
   d. For *Protocol*, select *HTTP*.
   e. For *Authentication Scheme*, select the authentication scheme that you created.

f. Disable *IP-based Authentication*.
g. Click *OK*.

Once you have configured an authentication scheme and rule, you can apply the user group that you created to a ZTNA policy to trigger user authentication.

Configuring ZTNA servers

ZTNA servers define the resources that you want ZTNA to allow access to. These resources are usually servers and applications that your FortiGate protects that you want to expose to your end users. ZTNA supports various TCP applications by creating TCP forwarding servers to map to. Alternatively, you can apply HTTP/HTTPS server mapping and use the HTTPS access proxy to directly map web requests to the web server without adding ZTNA connection rules

This example creates a ZTNA server mapping for connecting RDP to a server behind the FortiGate. For other ZTNA example configurations, see the *FortiOS Administration Guide*.

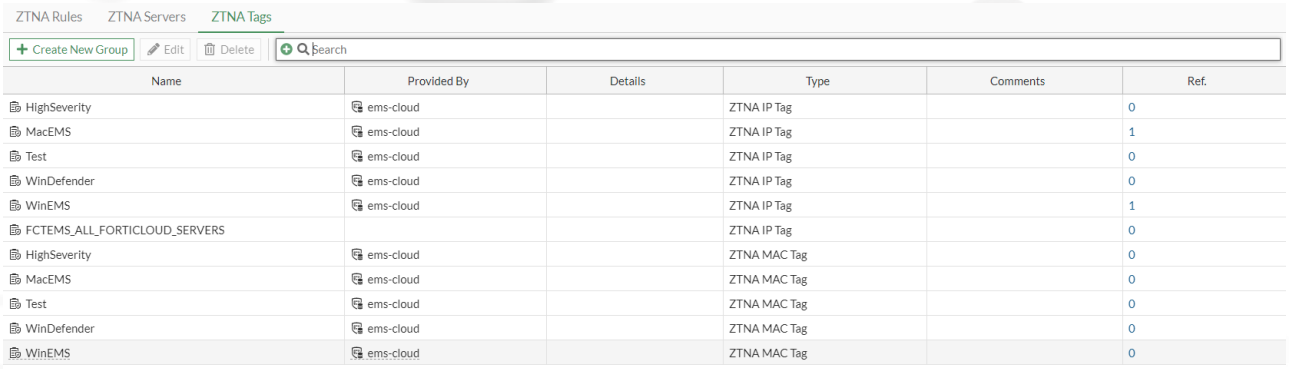
To configure a ZTNA server for mapping an RDP connection:

1. In FortiOS, go to *Policy & Objects > ZTNA > ZTNA Servers*.
2. Click *Create New*.
3. Under *Network*, choose the external interface, IP address, and port that users will connect to for the FortiGate access proxy.
4. If SAML authentication is used, enable the SAML option and select the server
5. Under *Services & Servers*, choose the default server certificate used to sign the connection to the FortiGate access proxy.
6. Configure the service mapping:
   a. Under *Service/Server mapping*, click *Create New*.
   b. For *Service type*, choose *TCP Forwarding*.
   c. Under *Servers*, click *Create New*. Configure the server:
      i. Enter the address of the server that you are mapping to.
      ii. For *Ports*, enter the port number of the service. For RDP, the default is 3389. Leaving the port empty allows mapping to all TCP ports.
   d. Click *OK* three times.

For additional TCP forwarding server mappings, create more servers under the TCP forwarding server mapping.

Configuring ZTNA policies

ZTNA policies define who can access what resources, and the security posture requirements for the device to be allowed access. You can select ZTNA tags that you created on FortiSASE here. You can view the tags in *Policy & Objects > ZTNA > ZTNA Tags*.



Name	Provided By	Details	Type	Comments	Ref.
HighSeverity	ems-cloud		ZTNA IP Tag		0
MacEMS	ems-cloud		ZTNA IP Tag		1
Test	ems-cloud		ZTNA IP Tag		0
WinDefender	ems-cloud		ZTNA IP Tag		0
WinEMS	ems-cloud		ZTNA IP Tag		1
FCTEMS_ALL_FORTICLOUD_SERVERS			ZTNA IP Tag		0
HighSeverity	ems-cloud		ZTNA MAC Tag		0
MacEMS	ems-cloud		ZTNA MAC Tag		0
Test	ems-cloud		ZTNA MAC Tag		0
WinDefender	ems-cloud		ZTNA MAC Tag		0
WinEMS	ems-cloud		ZTNA MAC Tag		0

This example denies access to a device that has a high or higher security vulnerability by detecting the presence of the HighSeverity tag. The example creates a second policy to grant access to devices that are secured with Windows Defender by detecting the presence of the WinDefender tag.

To create the deny policy:

1. Go to *Policy & Objects* > *ZTNA* > *ZTNA Rules*.
2. Click *Create New*.
3. In the *Incoming Interface* and *Source* fields, select the incoming interface and source.
4. In the *ZTNA Tag* field, select the HighSeverity ZTNA tag.
5. In the *ZTNA Server* field, select the ZTNA server that you created, and set the destination to *All*.
6. For *Action*, select *DENY*.
7. Enable *Log Violation Traffic*.
8. Click *OK*.

To create the allow policy:

1. Go to *Policy & Objects* > *ZTNA* > *ZTNA Rules*.
2. Click *Create New*.
3. Configure the policy:
   a. In the *Incoming Interface* and *Source* fields, enter the incoming interface and source.
   b. Under *Source*, add a user, and select the user group that you created.
   c. In the *ZTNA Tag* field, select the WinDefender ZTNA tag.
   d. In the *ZTNA Server* field, select the ZTNA server that you created.
   e. In the *Destination* field, select *All*.
   f. Keep the action as *Allow*.
   g. Configure the desired security profiles for scanning.
   h. Enable *Log Violation Traffic* for all sessions.
   i. Click *OK*.

You can create more policies as needed and move policies up and down on the *ZTNA Rules* page.

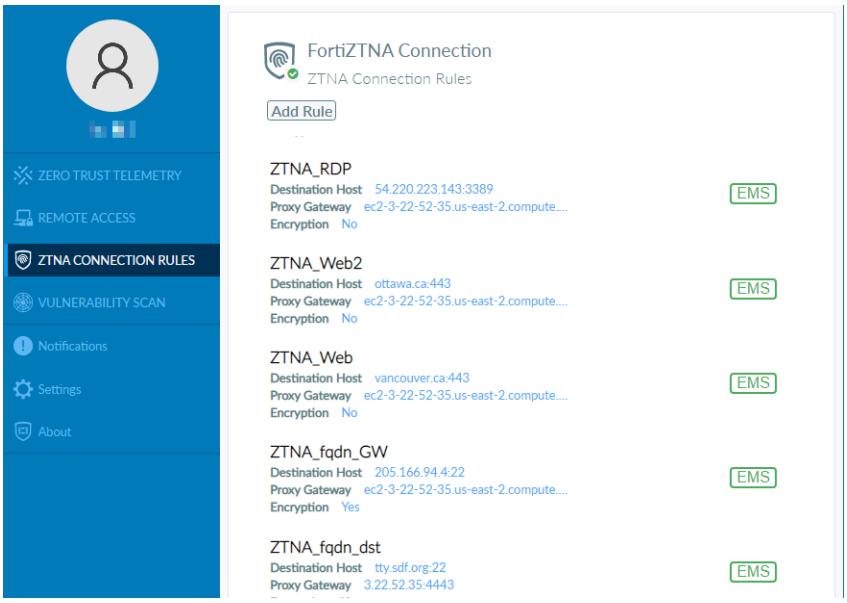
Configuring ZTNA connection rules on FortiSASE

When Zero Trust Network Access (ZTNA) TCP forwarding is used to map a server or application, you must add a corresponding ZTNA connection rule to the FortiClient endpoint to forward traffic to the FortiGate access proxy. You can create these rules on FortiSASE and push them to all managed endpoints.

To create a ZTNA connection rule on FortiSASE:

1. Go to *Configuration* > *Endpoints* > *Profile* > *ZTNA*.
2. Under *Connection Rules*, click *Create*. Configure the following:
   a. In the *Rule Name* field, enter a name to easily identify the mapped resource.
   b. In the *Destination Host* field, enter an IP address or FQDN of the remote device or application that you want to access, followed by the port. For example, you could enter 192.168.5.100:3389 or server.mydomain.com:3389.
   c. In the *ZTNA Access Proxy* field, enter the FortiGate access proxy IP address or FQDN and port, as defined in the FortiGate's ZTNA server settings. For example, you could enter ztnaproxy.mydomain.com:4443.
   d. Enable *Encryption* for insecure protocols. Disable *Encryption* for secure protocols.
   e. Enable *Use External Browser for SAML Authentication* only if SAML is used and you want to perform SAML authentication on an external browser instead of FortiClient's embedded browser.
   f. Click *OK*.
3. Click *Apply*.

FortiSASE pushes the ZTNA rules to managed endpoints via an endpoint profile update. Once updated, you can view the rules in FortiClient on the endpoint on the *ZTNA CONNECTION RULES* tab.



Configuring a split tunneling destination on FortiSASE

An endpoint can access private resources using zero trust network access (ZTNA) TCP forwarding when it has established a secure connection to FortiSASE. For FortiClient to forward this traffic directly to the FortiGate ZTNA access proxy without passing through FortiSASE, you must add a split tunneling destination corresponding to the IP or FQDN of the FortiGate. You can create this split tunneling destination on FortiSASE and push it to all managed endpoints.

To create a split tunneling destination on FortiSASE:

1. Go to *Configuration* > *Profiles*.
2. Select the *Default* profile and click *Edit*.

You cannot create subnet destinations in a custom endpoint profile. Therefore, subnet destinations defined in the Default profile also apply to all custom profiles.

3. On the *Access* tab, under *Bypass FortiSASE*, configure *Split tunneling destinations* by clicking *Create*. Configure the following:
   a. In the *Type* field, select *FQDN* or *Subnet* depending on whether you defined the *ZTNA Access Proxy* fields in the ZTNA connection rules using an FQDN or IP address.
   b. From the *Match* dropdown list, do one of the following:
      i. Select the FQDN host for the FQDN type.
      ii. Select the subnet host for the subnet type.
      If you have not created the FQDN or subnet host yet, click + to create a new FQDN or subnet host corresponding to the ZTNA access proxy.

FortiSASE does not support wildcard FQDNs when configuring an FQDN split tunneling destination.

   c. Click *OK*.
4. Configure additional split tunneling destinations corresponding to the ZTNA connection rules.
5. Click *Apply*. FortiSASE pushes the split tunnel destinations to managed endpoints via an endpoint profile update.

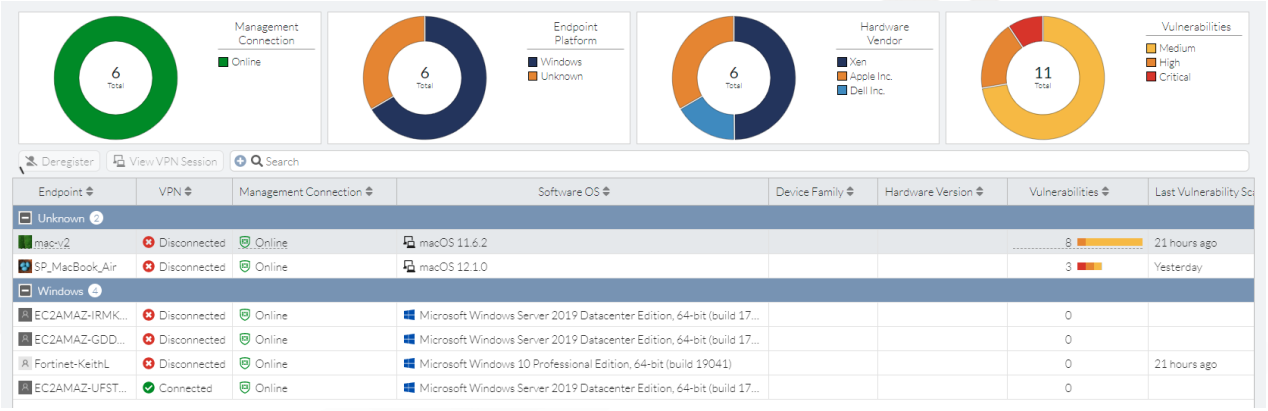
Testing and monitoring

You can test the configuration on a remote device.

To prepare the endpoint device:

1. Ensure that the end user received the onboarding email sent while configuring user authentication on FortiSASE.
2. After completing user activation, the user accesses the FortiSASE portal to download the appropriate FortiClient software.
3. Install the FortiClient software. During installation, select the Zero Trust Network Access (ZTNA) component.
4. After FortiClient launches, go to *ZERO TRUST TELEMETRY* and enter the invitation code. This triggers FortiClient to register to FortiSASE.

5. In FortiSASE, verify that the endpoint displays in *Configuration > Endpoints > Monitor*.



To verify the endpoint profile has been updated on the endpoint device:

Use the following steps to verify that the default endpoint profile configured in FortiSASE, which includes the ZTNA connection rules and split tunnel destination has been updated on the endpoint device.

1. In FortiClient, go to the *ZTNA DESTINATION* tab.
2. Ensure that the corresponding ZTNA connection rules configured in FortiSASE have been updated on the endpoint.
3. Open a Windows Command Prompt or PowerShell window with Administrator access.
4. In the Windows Command Prompt or PowerShell window, enter the following commands to confirm the split tunnel destination configured in FortiSASE has been updated on the endpoint:
   a. `ping access.ztnaproxy.com`, replacing `access.ztnaproxy.com` with your FortiGate ZTNA access proxy FQDN or IP address.
   b. `route print`

      In this output, you should find a route entry corresponding to the IP address of the FortiGate ZTNA access proxy determined in the previous command. For example, if the FortiGate ZTNA access proxy has an IP address of 1.1.1.1, and the endpoint has a FortiSASE VPN IP address of 10.212.128.1 and a private IP address to the internet router of 192.168.1.102 then you should see the following output:

```
C:\Users\Administrator> route print
...

IPv4 Route Table

===========================================================================
==
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     10.100.66.1    192.168.1.102     25
          0.0.0.0          0.0.0.0    10.212.128.2    10.212.128.1      2
...
          1.1.1.1  255.255.255.255     10.100.66.1   10.100.66.102    124
...
```

To connect to the FortiSASE gateway for internet access:

1. In FortiClient, go to the *REMOTE ACCESS* tab.
2. From the *VPN Name* dropdown list, select *FortiSASE SIA > Secure Internet Access*.
3. Enter the user credentials based on the VPN user authentication defined on FortiSASE. Click *Connect*.

4. Once connected, open a browser to go to websites as typical.
5. In FortiSASE, go to *Dashboard* > *FortiView* pages to monitor user traffic.
6. Go to *Configuration* > *Traffic* > *Security*. Click *View All* or *View Logs* for each security profile to drill down on traffic that each profile logged.

To connect to the FortiGate access proxy for ZTNA:

1. In FortiClient, go to the *ZTNA CONNECTION RULES* tab to view the list of servers and applications available through ZTNA TCP forwarding.
2. These instructions use RDP as an example. Open your Remote Desktop Connection console.
3. Enter the destination IP address or FQDN and port listed as the rule's destination host in the Remote Desktop Connection dialog. Click *Connect*.
4. FortiGate performs a device certificate check to verify the certificate validity and that the device is registered with FortiSASE.
5. If this is the first connection to the FortiGate access proxy, FortiClient prompts for user authentication. Enter your credentials to log in.
6. FortiGate performs security posture check by checking the endpoint's ZTNA tags and matching them against ZTNA policies. The first matching policy from the top determines whether this user and device is allowed access.
7. If everything passes, the user's traffic is forwarded to the RDP server. The user is prompted by the RDP to log in and continue with the connection.

To verify the ZTNA traffic logs on the FortiGate ZTNA access proxy:

1. Log in to the FortiGate.
2. Go to *Log & Report* > *ZTNA Traffic*.
3. Scroll through the log and look for the log entry corresponding to the RDP connection in the previous section.
4. Observe that the *Source* field contains the public or WAN IP address of the endpoint accessing the server using RDP. This confirms that the split tunneling destination was configured correctly and properly updated on the endpoint.
5. Observe that the *Real Server* field contains the private IP address corresponding to the server accessed using RDP.
6. Observe that the *Service* field displays RDP.

Appendix A - Products used in this guide

The following product models and firmware were used in this guide:

Product	Model	Firmware
FortiGate	VM	7.0.5
FortiClient	Windows	7.0.3

Appendix B - Documentation references

FortiSASE

- Authentication Sources and Access
- Configuring FortiSASE with an LDAP server for remote user authentication in FortiClient agent-based mode
- Configuring FortiSASE with a RADIUS server for remote user authentication
- Configuring FortiSASE with Azure Active Directory single sign on
- Security
- Endpoint Profile
- Tagging & Tagging Rules

FortiGate

- Zero Trust Network Access introduction
- Basic ZTNA configuration
- Establish device identity and trust context with FortiClient EMS
- SSL certificate based authentication
- ZTNA configuration examples

www.fortinet.com

72-242-997824-20240521